The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/22/2016

SUBJECT:
Multiple Vulnerabilities in phpMyAdmin Could Allow for Remote Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in phpMyAdmin, the most severe of which could result in remote code execution. Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- phpMyAdmin 4.6.x prior to 4.6.5
- phpMyAdmin 4.4.x prior to 4.4.15.9
- phpMyAdmin 4.0.x prior to 4.0.10.18

Note: Versions using the 4.4 branch no longer have security support after October 1, 2016 and no additional releases will be made available. Versions of the 4.0 branch will no longer have security support after April 1, 2017.

RISK:
Government:
- Large and medium government entities: **High**
- Small government: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:

Multiple vulnerabilities have been discovered in phpMyAdmin, the most severe of which could result in remote code execution. These vulnerabilities can be exploited if an attacker crafts and sends a malicious request to the affected application. Details of the vulnerabilities are as follows:

- A remote code execution vulnerability exists in the phpMyAdmin unserialize() function (CVE-2016-6620)
- A elevation of privilege vulnerability exists when the phpMyAdmin function PMA_safeUnserialize() function is manipulated with an unknown input (CVE-2016-9865)

Successful exploitation of these vulnerabilities could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:

- Upgrade to the latest version of phpMyAdmin immediately, after appropriate testing.
- Verify no unauthorized system modifications have occurred on system before applying patch.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Apply the principle of Least Privilege to all systems and services.

REFERENCES:

phpMyAdmin:
https://www.phpmyadmin.net/security/PMASA-2016-43/
https://www.phpmyadmin.net/security/PMASA-2016-70/

CVE:
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-6620
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2016-9865